Latest mass hacks highlight challenge for Biden administration

March 10 2021

Credit: CC0 Public Domain

The potentially devastating hack of Microsoft email servers, the second major cyberattack in months, adds pressure to the Biden administration as it weighs options for "hacking back" or other moves to protect cyberspace.

Security analysts say stronger actions are needed to deter the attacks which exploited vulnerabilities in corporate and government networks and opened opportunities for espionage and cybercrime.

The latest hack exploiting flaws in Microsoft Exchange service is believed to have affected at least 30,000 US organizations including local governments and was attributed to an "unusually aggressive" Chinese cyberespionage campaign.

The news comes on the heels of revelations that Russia was probably behind the massive SolarWinds hack that shook the government and corporate security last year.

"These are two very big incidents and represent a significant litmus test for the early stages of the Biden administration," said Frank Cilluffo, a former homeland security adviser in the George W. Bush administration who is now the director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security.

"A response is important because it sets a precedent and sets the tone for the administration's response to unacceptable cyber behavior."

Cilluffo added that any action would not simply respond to the perpetrators, noting that "everyone else is watching, and other state and nonstate actors are going to pay attention to our ability to respond."

James Lewis, a cybersecurity specialist with the Center for Strategic and International Studies, said the two incidents suggest "that our cybersecurity strategy isn't working against our most skilled and dangerous opponents."

"This means that the espionage advantages are endless," Lewis said. "The Biden team understands this and is trying to change things, but we are far

from having a solution."

Hacking back?

Until recently, the notion of "hacking back" counterstrikes was considered too politically risky under international norms. But a 2019 agreement among 28 countries set a legal framework for such retaliation, Lewis noted.

"Hacking back by private entities is still illegal, but the case has been made that it is legal for a state to do so in response to an attack," he said.

R. David Edelman, a former digital security adviser to the Obama administration who is now on the faculty at the Massachusetts Institute of Technology, said the new administration faces difficult choices

"The administration has said it wants to impose costs—and it's unclear what costs are commensurate. Just like with Solar Winds, the private sector is going to have to pay for another state's adventurism," Edelman said.

"Indictments? Sanctions? They only have so much effect when we're talking about agents safely ensconced in a foreign security state thousands of miles away."

'Surgical' response

Microsoft said a state-sponsored hacking group operating out of China is exploiting previously unknown security flaws in its Exchange email services to steal data from business users.

The hacking group, which it has named "Hafnium," is a "highly skilled

and sophisticated actor," according to the company.

This comes following revelations that hackers managed to compromise and instal malware on a piece of security software developed by SolarWinds which is used for management and supervision of networks at many large companies and several US government agencies.

The attack was discovered by cybersecurity company FireEye, which, along with SolarWinds, has pointed the finger at hackers linked to the Russian government.

Last month, Anne Neuberger, the senior White House cybersecurity advisor, said her team was looking "holistically" at retaliation.

"This isn't the only case of malicious cyber activity of likely Russian origin, either for us or for our allies and partners," she said.

Cilluffo said any response must be carefully crafted, like any military action, to punish the intended targets without harming innocent bystanders. That could mean economic, diplomatic or military measures, he said.

"This can't be treated as a cyber incident alone," he said. "It has to be woven into the broader geopolitical and national security machinery of the US government."

This could mean different kinds of responses for Russia, China, North Korea or others believed to be supporting hacker activity.

"A computer network attack is clearly an instrument in our toolbox," he said.

"But we want to do it surgically, discriminately and obviously have

impact on those we want to have impact on."